

ORM PTO-1	449			T OF COMMERCE DEMARK OFFICE	1573.101		1	10/028	1 of 1 on no. 265
					FIRST NAMED	-			
LIST OF	KEF	ERENCES C	I I ED BA	APPLICANT	Koichi IT	O, et al.		ROUP AR	71007
	(Us	e several sheets	if necessar	y)		er 28, 2001	- 1	2131	TORIT
			11.0.0	ATENT DOCUME					<u>, , , , , , , , , , , , , , , , , , , </u>
EXAMINER	Τ	DOCUMENT	U.S. PA	ATENT DOCUME	NIS	1		JB-	FILING
INITIAL		NO.	DATE	NAME		CLASS	CU	SS	DATE
TMS	AA	5,452,358	09/1995	Normile et al.			1-		
<u> </u>	AB					RE	CEIV	ED	
	AC					AU	G 1 4	2003	
	AD					Technol	ogy Cen	ter 210	0
	AE						•		
	AF								
<u>-</u>			FOREICA	PATENT DOCU	MENTS				
		DOCUMENT	FOREIGN				SUB-		NSLATION
		NO.	DATE	COUNTR		CLASS	CLASS	YE	S NO
1.MC	AG	0 981 223 A2	02/2000	European Paten	t Office				
1MS	AH	0 792 041 A2	08/1997	European Paten	t Office				
	Al					,	•		·
	AJ								
	AK				_ :				
	AL						-		
THER RE	FERE	NCES (Including	Author, T	itle, Date, Pertine	ent Pages,	Etc.)			ANSLATIC ES NO
(ms	AM	Analysis Attack	ks", PROCE	Securing the AES EEDINGS OF FAS OP 2000, April 10	T SOFTW	ARE			
XAMINER		h I		DATE	CONSIDER	RED			

(D	IPE
FEB (1 2007 85
THE STATE OF THE S	
40 /4 >	- 10/11 c

ORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY DOCKET NO. | AF | 1573.1010 | 1

Sheet 1 of 2 APPLICATION NO. 10/028,265

LIST OF REFERENCES CITED BY APPLICANT

FILING DATE

Koichi ITO, et al.

FIRST NAMED INVENTOR

GROUP ART UNIT

(Use several sheets if necessary)

December 28, 2001

*EXAMINER INITIAL	DOCUMENT NO.	DATE	NAME	CLASS	SUB- CLASS	FILING DATE
A	\					
Al	3	 				
A						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB- CLASS	TRANSL YES	ATION NO
TMS	AD	2000-305453	11/2000	Japan			Х	
1	AE	WO 99/67919	12/1999	WIPO)	Х	
	AF	WO 00/46953	08/2000	WIPO	_	•	Х	
	AG	WO 00/27068	05/2000	WIPO)	Х	
	AH	WO 00/49765	08/2000	WIPO		-	Х	
	Al	WO 01/10077.	02/2001	WIPO			Х	

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)

—		
1MS	AJ	Kocker, Paul, et al., "Differential Power Analysis" in Proceedings of Advances in
$ l^{\vee \vee} \rangle$		Cryptology-CRYPTO '99, Springer-Verlag 1999. pages 388-397.
1	AK	Messerges, Thomas, et al., "Power Analysis Attacks of Modular Exponentiation in
		Smartcards", Cryptographic Hardware and Embedded Systems (CHES '99), Springer-
.		Verlag, pages 144-157
	AL	Akkar, Mehdi-Laurent, et al., "Power Analysis, What is Now Possible", ASIACRYPT
1 1		2000, Pages 489-502.
<i>i</i> 1 ,	AM	Messerges, Thomas S., "Securing the AES Finalists Against Power Analysis Attacks",
$\perp \Psi$	1	Proceedings of Fast Software Encryption Workshop 2000, Springer-Verlag, April 2000,
~	1	which is called "a masking method."

		DATE CONSIDERED
Ay/	1	10/4/05
	dy/	dy

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Sheet 2 of 2

FORM PTO-1449

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

ATTORNEY DOCKET NO. 1573.1010 APPLICATION NO. 10/028,265
FIRST NAMED INVENTOR

LIST OF REFERENCES CITED BY APPLICANT

(Use several sheets if necessary)

Koichi ITO, et al.

FILING DATE
December 28, 2001

GROUP ART UNIT

U.S. PATENT DOCUMENTS

*EXAMINER INITIAL		DOCUMENT NO.	DATE	NAME	CLASS	SUB- CLASS	FILING DATE
	ВА						".
	ВВ						
	ВС						
	BD						
	BE						
	BF						

FOREIGN PATENT DOCUMENTS

		DOCUMENT NO.	DATE	COUNTRY	CLASS	SUB- CLASS	TRANS! YES	LATION NO
1 Ms	BG	WO 00/24155	04/2000	WIPO		١.	Х	
1m5	вн	WO 00/24156	04/2000	WIPO			Х	
	ВІ							
	BJ			·				
	вк							
	BL							

OTHER REFERENCES (Including Author, Title, Date, Pertinent Pages, Etc.)

			STITELY RELEASED (Mondaing Adults, Timo, Date, Fortillorit ages, Els.)
1	145	вм	Messerges, Thomas S. et al., "Investigations of Power Analysis Attacks on Smartcards", Proceedings of USENIX Workshop on Smartcard Technology, March 1999.
		BN	Chari, Suresh, et al., "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards", Second Advanced Encryption Standard Candidate Conference, March 1999.
		во	FIPS 46, "Data Encryption Standard" Federal Information Processing Standards Publication 46, U.S. Departement of Commerce/National Bureau of Standards, National Technical Information Service, Springfield, VA, 1977.
,		ВР	http://csrc.nist.gove/encryption/aes/rijndael/Rijndael.pdf (which is linked from http://www.nist.gov/aes/).

EXAMINER MINING	DATE CONSIDERED	10/4/05
*EXAMINER: Initial if reference considered, whether of not citation	is in conformance with MPEP 6	09: Draw line through citation if